Please Update Your Niagara Software to Address QNX BadAlloc and Privilege Escalation Vulnerabilities as well as JxBrowser Vulnerability

Security Bulletin #: SB 2021-Tridium-2 and SB 2021-Tridium-3

Defect#: PSIRT-734
CVSSv3: 3.9 (AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L)

Defect#: PSIRT-691
CVSSv3: 4.3 (AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N)

Defect#: PSIRT-696- HCECBFEASEC-48
CVSSv3: 6.6 (AV:A/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)

Defect#: PSIRT-696- HCECBFEASEC-49
CVSSv3: 2.0 (AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N)

Summary

This bulletin is to make you aware of a few recently reported vulnerabilities:

- Blackberry QNX has revealed an integer overflow that impacts QNX OS version 6.50 SP1 and earlier (CVE-2021-22156). To learn more about this vulnerability known as Bad Alloc, see the CISA Alert. All QNX-based Niagara Framework® platforms prior to Niagara 4.8 are impacted. (Niagara Edge® 10 releases are not exposed.) Due to compensating controls in Niagara, the CVSS score for this vulnerability has been recalculated to be 3.9 and is classified as a low risk.
- A medium-level Privilege Escalation vulnerability has been identified in QNX code used in Niagara platforms prior to Niagara 4.10u1. Exploitation of this vulnerability does not expose any additional functionality or data. An update has been made to Niagara platforms to mitigate this vulnerability.
- In addition, a handful of vulnerabilities were identified in the Chromium version embedded in jxBrowser. All Niagara-based platforms prior to Niagara 4.10u1 are impacted.

Recommended Action

Tridium recommends upgrading to Niagara 4.10u1 and Niagara EntSec 4.10u1. These updates are available by contacting your sales support channel or by contacting the Tridium support team at support@tridium.com

It is important that all Niagara customers for all supported platforms update their systems with these releases to mitigate risk. If you have any questions, please contact your Tridium account manager or Customer Support at support@tridium.com. As always, we highly recommend that Niagara customers running on unsupported platforms (such as Niagara AX) take action to update their systems to a supported platform, ideally the 4.10u1 release of Niagara Framework or the 4.10u1 release of Niagara Enterprise Security.

Mitigation

In addition to updating your system, Tridium recommends that customers with affected products take the following steps to protect themselves:

- Review and validate the list of users who are authorized and who can authenticate to Niagara.
- Allow only trained and trusted persons to have physical access to the system, including devices that have connection to the system though the Ethernet port.
- Consider using a VPN or other means to ensure secure remote connections into the network where the system is located, If remote connections are enabled,
- Sign all modules and program objects provided by third-party teams.

- Review the Niagara Hardening Guide for techniques on securing your installation.

Cybersecurity is a priority at Tridium. We are dedicated to continuously improving the security of our products, and we will continue to update you as we release new security features, enhancements, and updates.

Acknowledgement

Tridium would like to acknowledge the following researchers from PeopleTec (www.peopletec.com) for their help identifying this set of vulnerabilities and reporting them to us: Joel Sanchez, Todd Heflin and Tracy Williams.

In addition, Tridium would also like to acknowledge the following researchers i identify this vulnerability and reporting it to us: Martino Tommasini Carl Dworzack and Rick de Jager.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION IN THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- TRIDIUM RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- TRIDIUM PROVIDES THE CVSS SCORES 'AS IS' WITHOUT WARRANTY OF ANY KIND. TRIDIUM DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL TRIDIUM BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT. SPECIAL, OR CONSEQUENTIAL DAMAGES.

September 2021